

1 TINA WOLFSON, SBN 174806  
2 [twolfson@ahdootwolfson.com](mailto:twolfson@ahdootwolfson.com)  
3 ROBERT AHDOOT, SBN 172098  
4 [rahdoot@ahdootwolfson.com](mailto:rahdoot@ahdootwolfson.com)  
5 THEODORE W. MAYA, SBN 223242  
6 [tmaya@ahdootwolfson.com](mailto:tmaya@ahdootwolfson.com)  
7 KEITH CUSTIS, SBN 218818 (Of Counsel)  
8 [keith@custis-law.com](mailto:keith@custis-law.com)

**AHDOOT & WOLFSON, P.C.**

9  
10 1016 Palm Street  
11 West Hollywood, California 90069  
12 Tel: 310-474-9111; Fax: 310-474-8585

13 JOHN A. YANCHUNIS (Pro Hac Vice  
14 application to be filed)

15 [jyanchunis@forthepeople.com](mailto:jyanchunis@forthepeople.com)

16 **MORGAN & MORGAN**  
17 201 N. Franklin Street, 7th Floor  
18 Tampa, Florida 33602

19 Tel: (813) 223-5505; Fax: (813) 223-5402

20 Counsel for Plaintiffs

21 WALID KHALAF, JASMIN GONZALEZ,  
22 STEFANIE SMITH and STEVE O'BRIEN

PAUL C. WHALEN (Pro Hac Vice  
application to be filed)

[pcwhalen@gmail.com](mailto:pcwhalen@gmail.com)

**LAW OFFICES OF PAUL C.  
WHALEN, P.C.**

768 Plandome Road  
Manhasset, New York 11030

Tel: (516) 627-5610; Fax: (212) 658-9685

17 **UNITED STATES DISTRICT COURT**

18 **SOUTHERN DISTRICT OF CALIFORNIA**

20 WALID KHALAF, JASMIN GONZALEZ,  
21 STEFANIE SMITH and STEVE O'BRIEN,  
22 individually and on behalf of all others  
similarly situated,

Case No. '14CV2175 GPC JMA

**CLASS ACTION COMPLAINT**

JURY TRIAL DEMANDED

23 Plaintiffs,

24 v.

26 HOME DEPOT U.S.A., INC., a Delaware  
27 corporation,

28 Defendant.

1 Plaintiffs Walid Khalaf, Jasmin Gonzalez, Stefanie Smith and Steve O'Brien, by  
 2 and through their counsel, bring this Class Action Complaint against defendant Home  
 3 Depot U.S.A., Inc., on behalf of themselves and all others similarly situated, and allege,  
 4 upon personal knowledge as to their own actions and their counsel's investigations, and  
 5 upon information and belief as to all other matters, as follows:

6 **NATURE OF THE ACTION**

7 1. Plaintiffs bring this class action against Defendant Home Depot U.S.A.,  
 8 Inc. for its failure to secure and safeguard its customers' credit and debit card numbers  
 9 and other payment card data ("PCD"), personally identifiable information such as the  
 10 cardholder's names, mailing addresses, and other personal information ("PII")  
 11 (collectively, "Private Information"), and for failing to provide timely and adequate  
 12 notice to Plaintiffs and other Class members that their Private Information had been  
 13 stolen and precisely what types of information were stolen.

14 2. Beginning in or around April 2014, hackers utilizing malicious software  
 15 accessed the point-of-sale systems at Home Depot locations throughout the United  
 16 States and stole copies of Home Depot customers' Private Information (the "Data  
 17 Breach"). In early September 2014, Home Depot customers' Private Information was  
 18 placed for sale on an underground website notorious for offering PII and PCD.

19 3. On September 3, 2014, after security blogger Brian Krebs first reported  
 20 news of the Data Breach, Home Depot admitted that it did not become aware of the  
 21 Data Breach until September 2, 2014. Six days later, on September 8, 2014, Home  
 22 Depot confirmed on its website that it had allowed a massive breach of its customers'  
 23 Private Information to occur in 2014, stating that its "systems have in fact been  
 24 breached, which could potentially impact any customer that has used their payment card  
 25 at our U.S. and Canadian stores, from April forward."<sup>1</sup> Home Depot's security  
 26 protocols were so deficient that the Data Breach continued for nearly five months while

27  
 28 <sup>1</sup> <<https://corporate.homedepot.com/mediacenter/pages/statement1.aspx>> (last visited  
 Sept. 12, 2014).

1 Home Depot failed to even detect it – this despite widespread knowledge of the  
 2 malicious software (or malware) used to perpetrate the Data Breach, which was a  
 3 variant of the same malware used to perpetrate an earlier, notorious, and widely  
 4 reported data breach affecting the retailer Target Corporation.<sup>2</sup>

5       4. Home Depot has yet to fully disclose what types of Private Information  
 6 were stolen, but concedes that “[p]ayment card information such as name, credit card  
 7 number, expiration date, cardholder verification value and service code for purchases  
 8 made at Home Depot stores in 2014, from April on” were “compromised.”<sup>3</sup>

9       5. Reuters reports that “experts fear the attackers may have gotten away with  
 10 more than 40 million payment cards, which would exceed the number taken in last  
 11 year’s unprecedented data breach on Target Corp.”<sup>4</sup> Home Depot concedes that  
 12 customers who shopped at its stores as far back as April 2014 were exposed. Thus, the  
 13 Data Breach extended for nearly five months, including the busy summer season — far  
 14 longer than the three-week Target data breach.

15       6. Home Depot could have prevented this Data Breach. The malicious  
 16 software used in the Data Breach was a variant of “BlackPOS,” the identical malware  
 17 strain that hackers used in last year’s data breach at Target. While many retailers, banks  
 18 and card companies responded to recent breaches, including the Target breach, by  
 19 adopting technology that helps makes transactions more secure, Home Depot did not do  
 20 so.

21       7. Home Depot disregarded Plaintiffs’ and Class members’ rights by  
 22 intentionally, willfully, recklessly, or negligently failing to take adequate and  
 23 reasonable measures to ensure its data systems were protected, failing to take available

---

24  
 25 <sup>2</sup> <<http://krebsonsecurity.com/2014/09/home-depot-hit-by-same-malware-as-target/>>  
 26 (last visited Sept. 12, 2014).

27 <sup>3</sup> <<https://corporate.homedepot.com/MediaCenter/Documents/Required%20Regulatory%20Notice.PDF>> (last visited Sept. 12, 2014).

28 <sup>4</sup> <<http://www.reuters.com/article/2014/09/09/home-depot-dataprotection-breach-probe-idUSL1N0RA1DL20140909>> (last visited Sept. 12, 2014).

1 steps to prevent and stop the breach from ever happening, and failing to disclose to its  
2 customers the material facts that it did not have adequate computer systems and security  
3 practices to safeguard customers' Private Information. On information and belief,  
4 Plaintiffs' and Class members' Private Information was improperly handled and stored,  
5 was unencrypted, and was not kept in accordance with applicable, required, and  
6 appropriate cyber-security protocols, policies, and procedures. As a result, Plaintiffs'  
7 and Class members' Private Information was compromised and stolen.

8. Plaintiffs bring this lawsuit on behalf of themselves and all others  
9 similarly situated, alleging that Home Depot violated the California Consumer Records  
10 Act, Civil Code Sections 1798.81.5 & 1798.82; breached its implied contract with  
11 Plaintiffs and Class members; and violated the California's Unfair Competition Law,  
12 Cal. Bus. & Prof. Code § 17200, *et seq.* ("UCL").

### 13 **PARTIES**

14. Plaintiff Walid Khalaf is an individual and resident of San Diego County,  
15 California. Between April 1, 2014 and September 8, 2014, Mr. Khalaf used a credit card  
16 to make several purchases at the Home Depot store located at 5920 Fairmount Ave, San  
17 Diego, California. To date, Mr. Khalaf has not received any notice from Home Depot  
18 about the Data Breach.

19. Plaintiff Jasmin Gonzalez is an individual and resident of Los Angeles  
20 County, California. Between April 1, 2014 and September 8, 2014, Ms. Gonzalez used  
21 a credit card to make several purchases at the Home Depot store located 2450 Cherry  
22 Avenue, Signal Hill, California. To date, Ms. Gonzalez has not received any notice  
23 from Home Depot about the Data Breach.

24. Plaintiff Stefanie Smith is an individual and resident of Los Angeles  
25 County, California. Between April 1, 2014 and September 8, 2014, Ms. Smith used a  
26 Bank of America debit card to make five purchases at the Home Depot store located at  
27 5000 Hardwick St., Lakewood, California, including a purchase on September 4, 2014.  
28 To date, Ms. Smith has not received any notice from Home Depot about the Data

1 Breach.

2 12. Plaintiff Steve O'Brien is an individual and resident of San Diego County,  
3 California. Between April 1, 2014 and September 8, 2014, Mr. O'Brien used a credit  
4 card to make several purchases at the Home Depot store located at 3555 Sports Arena  
5 Blvd, San Diego, California. To date, Mr. O'Brien has not received any notice from  
6 Home Depot about the Data Breach.

7 13. Home Depot Home Depot U.S.A., Inc. is a Delaware corporation  
8 headquartered in Atlanta, Georgia. Home Depot operates retail stores throughout the  
9 United States, including the California locations where Plaintiffs' purchases were made.

10 **JURISDICTION AND VENUE**

11 14. This Court has jurisdiction over this action under the Class Action Fairness  
12 Act, 28 U.S.C. § 1332(d). The aggregated claims of the individual class members  
13 exceed \$5,000,000, exclusive of interest and costs, and this is a class action in which  
14 more than two-thirds of the proposed plaintiff class, on the one hand, and defendant  
15 Home Depot, on the other, are citizens of different states.

16 15. This Court has jurisdiction over Home Depot because it is registered to  
17 conduct business in California, has sufficient minimum contacts in California or  
18 otherwise intentionally avails itself of the markets within California, through the  
19 promotion, sale, marketing and distribution of products sold at its retail stores located in  
20 California, to render the exercise of jurisdiction by this Court proper and necessary.

21 16. Venue is proper in this District pursuant to 28 U.S.C. § 1331(a)(1) because  
22 a substantial part of the events and omissions giving rise to this action occurred in this  
23 District as Home Depot operates retail locations within this District, Plaintiff Khalaf  
24 resides here, and his purchases took place at Home Depot's retail store located within  
25 this District.

26 //

27 //

28 //

## **FACTUAL BACKGROUND**

## A. Home Depot and its Private Information Collection Practices

17. Home Depot operates approximately 1,977 home improvement and construction retail stores in the United States. Home Depot is the fifth largest retailer in the United States, behind Walmart, Kroger, Costco, and Target, with annual U.S. sales in 2013 of \$69,951 billion.

18. When consumers make purchases at Home Depot retail stores using credit or debit cards, Home Depot collects PCD related to that card including the card holder name, the account number, expiration date, card verification value (CVV), and PIN data for debit cards. Home Depot stores the PCD in its point-of-sale system and transmits this information to a third party for completion of the payment. Home Depot also collects and stores PII, including but not limited to customer names, mailing addresses, phone numbers, and email addresses.

19. Through its Privacy Policy, which is available on its website, Home Depot advises consumers about the categories of Private Information it collects:

## Information We Collect

## Contact information

We may collect the names and user names of our customers and other visitors. Additionally, we may collect your purchase history, billing and shipping addresses, phone numbers, email addresses, and other digital contact information. We may also collect information that you provide us about others.

## Payment information

When you make a purchase we collect your payment information, including information from your credit or debit card, check, PayPal account or gift card. If you apply for a The Home Depot credit card or a home improvement loan, we might collect information related to your application.

## Returns information

When you return a product to our stores or request a refund or exchange, we may collect information from you and ask you

1 to provide your government issued ID. We use the  
 2 information we collect from you and capture off of your  
 3 government issued ID to help prevent fraud. To learn more  
 4 about our Returns Policy, click here.

5 **Demographic information**

6 We may collect information about products or services you  
 7 like, reviews you submit, or where you shop. We might also  
 8 collect information like your age or gender.

9 **Location information**

10 If you use our mobile websites or applications, we may collect  
 11 location data obtained from your mobile device's GPS. If you  
 12 use our websites, we may collect location data obtained from  
 13 your IP address. We use this location data to find our nearest  
 14 store to you, product availability at our stores near you and  
 15 driving directions to our stores.

16 **Other information**

17 If you use our websites, we may collect information about the  
 18 browser you are using. We might track the pages you visit,  
 19 look at what website you came from, or what website you  
 20 visit when you leave us. We collect this information using the  
 21 tracking tools described here. To control those tools, please  
 22 read the Your Privacy Preferences section.<sup>5</sup>

23 20. Thus, Home Depot stores massive amounts of PII and PCD on its servers  
 24 and utilizes this information to maximize its profits through predictive marketing and  
 25 other marketing techniques.

26 **B. Consumers Rely On Home Depot's Private Information Security Practices**

27 21. Consumers place value in data privacy and security, and they consider it  
 28 when making purchasing decisions. Plaintiffs would not have made purchases at Home  
 29 Depot, or would not have paid as much for them, had they known that Home Depot  
 30 does not take all necessary precautions to secure their personal and financial data.  
 31 Home Depot failed to disclose its negligent and insufficient data security practices and  
 32 consumers relied on this omission to make purchases at Home Depot.

---

25 <sup>5</sup> <[http://www.homedepot.com/c/Privacy\\_Security](http://www.homedepot.com/c/Privacy_Security)> (hyperlinks omitted) (last visited  
 26 Sept. 12, 2014).

1       22. Furthermore, when consumers purchase goods at a national retailer, such  
 2 as Home Depot, they assume that its data security practices and policies are state-of-  
 3 the-art and that the retailer will use part of the purchase price that consumers pay for  
 4 such state-of-the-art practices. Consumers thus enter into an implied contract with  
 5 Home Depot that Home Depot will adequately secure and protect their Private  
 6 Information, and will use part of the purchase price of the goods to pay for adequate  
 7 data security measures. In fact, rather than use those moneys to implement adequate  
 8 data security policies and procedures, Home Depot failed to provide reasonable security  
 9 measures, thereby breaching its implied contract with Plaintiffs.

10 **C. Stolen Private Information Is Valuable to Hackers and Thieves**

11       23. It is well known and the subject of many media reports that PII data is  
 12 highly coveted and a frequent target of hackers. PII data is often easily taken because it  
 13 may be less protected and regulated than payment card data.

14       24. Legitimate organizations and the criminal underground alike recognize the  
 15 value in PII. Otherwise, they wouldn't pay for it or aggressively seek it. For example,  
 16 in "one of 2013's largest breaches . . . not only did hackers compromise the [card holder  
 17 data] of three million customers, they also took registration data from 38 million  
 18 users."<sup>6</sup> Similarly, in the Target data breach, in addition to PCI data pertaining to  
 19 40,000 credit and debit cards, hackers stole PII pertaining to 70,000 customers.

20       25. "Increasingly, criminals are using biographical data gained from multiple  
 21 sources to perpetrate more and larger thefts." *Id.*

22       26. PII data has been stolen and sold by the criminal underground on many  
 23 occasions in the past, and the accounts of thefts and unauthorized access have been the  
 24 subject of many media reports. Unfortunately, and as will be alleged below, despite all  
 25 of this publicly available knowledge of the continued compromises of PII in the hands

26  
 27       

---

<sup>6</sup> Verizon 2014 PCI Compliance Report, available at <[http://www.nocash.info.ro/wp-content/uploads/2014/02/Verizon\\_pci-report-2014.pdf](http://www.nocash.info.ro/wp-content/uploads/2014/02/Verizon_pci-report-2014.pdf)> (hereafter "2014 Verizon Report"), at 54 (last visited Sept. 12, 2014).

1 of other third parties, such as retailers, Home Depot's approach at maintaining the  
 2 privacy of Plaintiffs' and Class members' PII was lackadaisical, cavalier, reckless, or at  
 3 the very least, negligent.

4 **D. Home Depot Failed to Segregate PCD From PII**

5 27. Unlike PII data, PCD (or payment card data) is heavily regulated. The  
 6 Payment Card Industry Data Security Standard ("PCI DSS") is a set of requirements  
 7 designed to ensure that companies maintain consumer credit and debit card information  
 8 in a secure environment.

9 28. "PCI DSS provides a baseline of technical and operational requirements  
 10 designed to protect cardholder data."<sup>7</sup>

11 29. One PCI requirement is to protect stored cardholder data. Cardholder data  
 12 includes Primary Account Number, Cardholder Name, Expiration Date, and Service  
 13 Code.

14 30. "Network segmentation of, or isolating (segmenting), the cardholder data  
 15 environment from the remainder of an entity's network is not a PCI DSS requirement."<sup>8</sup>  
 16 However, segregation is recommended because among other reasons, "[i]t's not just  
 17 cardholder data that's important; criminals are also after personally identifiable  
 18 information (PII) and corporate data."<sup>9</sup>

19 31. Illicitly obtained PII and PCI, sometimes aggregated from different data  
 20 breaches, is sold on the black market, including on websites, as a product at a set  
 21 price.<sup>10</sup>

22 **E. The 2014 Data Breach at Home Depot**

23 32. On September 2, 2014, Home Depot's banking partners and law

---

25 <sup>7</sup> PCI DSS v. 2 at 5 (2010) (hereafter PCI Version 2).

26 <sup>8</sup> *Id.* at 10.

27 <sup>9</sup> See Verizon Report at 54.

28 <sup>10</sup> See, e.g., <<http://krebsonsecurity.com/2011/11/how-much-is-your-identity-worth>>  
 (last visited Sept. 12, 2014).

1 enforcement officials notified the retailer of a potential data breach involving the theft  
 2 of its customers' credit card and debit card data.

3       33. That same day, multiple banks began reporting evidence that Home Depot  
 4 stores were the likely source of a massive batch of stolen card data that went on sale  
 5 that morning at rescator.cc, the same underground cybercrime shop that sold millions of  
 6 cards stolen in the 2013 attack on Target.<sup>11</sup>

7       34. Specifically, according to security blogger Brian Krebs of Krebs on  
 8 Security (the "Krebs Report"), the cybercrime store rescator.cc (the "Rescator website")  
 9 listed consumer credit cards for sale that, with the unique ZIP code and other card data,  
 10 at least four banks had traced back to previous transactions at Home Depot.

11       35. The Krebs Report explained that "experienced crooks prefer to purchase  
 12 cards that were stolen from stores near them, because they know that using the cards for  
 13 fraudulent purchases in the same geographic area as the legitimate cardholder is less  
 14 likely to trigger alerts about suspicious transactions — alerts that could render the stolen  
 15 card data worthless for the thieves."<sup>12</sup> The Krebs Report indicated a "staggering 99.4  
 16 percent overlap" between the unique ZIP codes represented on the Rescator website and  
 17 those of Home Depot stores, strongly suggesting that the source of the breached credit  
 18 card data was from Home Depot.

19       36. The ZIP code information the Krebs Report pulled from the Rescator  
 20 website appears to represent the vast majority, if not all, of Home Depot's  
 21 approximately 2,000 domestic retail locations. The Krebs Report further indicated that,  
 22 based on conversations with affected banks, this data breach "probably started in late  
 23 April or early May" and may be ongoing, potentially dwarfing the 40 million debit and  
 24 credit cards affected by the recent Target data breach (which had 1,800 stores affected

25  
 26       <sup>11</sup> <<http://krebsonsecurity.com/2014/09/home-depot-hit-by-same-malware-as-target/>>  
 27 (last visited Sept. 12, 2014).

28       <sup>12</sup> <<http://krebsonsecurity.com/2014/09/data-nearly-all-u-s-home-depot-stores-hit/>> (last  
 visited Sept. 12, 2013).

1 during a period of approximately 3 weeks).

2 37. On September 3, 2014, Home Depot could not confirm whether a data  
 3 breach occurred, but indicated it first learned of a “potential breach” on September 2,  
 4 2014, at least one day before the Krebs Report.<sup>13</sup>

5 38. Indeed, after this news broke, Home Depot released an ambiguous and  
 6 uninformative statement buried on its corporate site – and not the Internet site visited by  
 7 consumers – concerning the Data Breach that failed to confirm the breach, and still did  
 8 not notify affected customers directly:

9 **Message to our customers about news reports of a possible  
 10 payment data breach.**

11 We’re looking into some unusual activity that might indicate a  
 12 possible payment data breach and we’re working with our  
 13 banking partners and law enforcement to investigate. We  
 14 know that this news may be concerning and we apologize for  
 15 the worry this can create. If we confirm a breach has  
 16 occurred, we will make sure our customers are notified  
 17 immediately.<sup>14</sup>

18 39. On September 8, 2014, Home Depot confirmed that its systems “have in  
 19 fact been breached, which could potentially impact any customer that has used their  
 20 payment card at our U.S. and Canadian stores, from April forward.”<sup>15</sup>

21 40. Home Depot has not indicated whether social security numbers, PIN  
 22 numbers and dates of birth were compromised, nor has it disclosed whether the wide  
 23 range of other PII that it collects, including names, addresses, telephone numbers,  
 24 mobile telephone numbers, driver’s license numbers, bank account numbers, email  
 25 addresses, computer IP addresses, and location information, were disclosed in the

---

26 <sup>13</sup> <<http://online.wsj.com/articles/home-depot-tries-to-reassure-customers-about-possible-data-breach-1409743851>> (last visited Sept. 12, 2014).

27 <sup>14</sup> <<https://corporate.homedepot.com/mediacenter/pages/statement1.aspx>> (last visited Sept. 12, 2014).

28 <sup>15</sup> <<https://corporate.homedepot.com/mediacenter/pages/statement1.aspx>> (last visited Sept. 12, 2014).

1 breach.<sup>16</sup>

2 41. Without such detailed disclosure, Plaintiffs and Class members are unable  
3 to take the necessary precautions to prevent imminent harm, such as continued misuse  
4 of their personal information.

5 42. If fraud were occurring from late April to early September of 2014,  
6 because hackers already had their hands on cardholder data and PII, credit card  
7 company analytics and other methods (undercover investigations of the black market)  
8 would likely have discovered it before September 2, 2014. Home Depot has failed to  
9 provide a cogent picture of how the Data Breach occurred and its full effects on  
10 customers' PII and PCD information.

11 43. Hacking is often accomplished in a series of phases to include  
12 reconnaissance, scanning for vulnerabilities and enumeration of the network, gaining  
13 access, escalation of user, computer and network privileges, maintaining access,  
14 covering tracks and placing backdoors. On information and belief, while hackers  
15 scoured Home Depot's networks to find a way to access PCD, they had access to and  
16 collected the PII stored on Home Depot's networks.

17 44. "The stolen card data being offered for sale on rescator.cc includes both  
18 the information needed to fabricate counterfeit cards *as well as the legitimate*  
19 *cardholder's full name* and the city, state and ZIP of the Home Depot store from which  
20 the card was stolen."<sup>17</sup> Information pertaining to the cardholder's location allows  
21 hackers to obtain a cardholder's Social Security number and date of birth, further  
22 increasing the risk of identity theft (above and beyond fraudulent credit and/or debit  
23 card transactions) for affected Home Depot customers.

24 45. Thieves already are using the Private Information stolen from Home Depot  
25 to commit actual fraud. Some thieves are using the Private Information to change a  
26

---

27 <sup>16</sup> <[http://www.homedepot.com/c/Privacy\\_Security](http://www.homedepot.com/c/Privacy_Security)> (last visited Sept. 12, 2014).

28 <sup>17</sup> <<http://krebsonsecurity.com/2014/09/in-wake-of-confirmed-breach-at-home-depot-banks-see-spike-in-pin-debit-card-fraud/>> (last visited Sept. 12, 2014).

1 cardholder's PIN numbers on stolen debit cards and to make ATM withdrawals from  
 2 Home Depot customer's accounts. On September 8, 2014, a bank located on the West  
 3 Coast reported that it "lost more than \$300,000 in two hours today to PIN fraud on  
 4 *multiple debit cards that had all been used recently at Home Depot.*"<sup>18</sup> (emphasis  
 5 added). On that same day, the Krebs Report advised that multiple financial institutions  
 6 had reported "a steep increase over the past few days in fraudulent ATM withdrawals  
 7 on customer accounts."

8       46. The Data Breach was caused and enabled by Home Depot's knowing  
 9 violation of its obligations to abide by best practices and industry standards in  
 10 protecting its customers' Private Information.

11       47. In this regard, the software used in the attack was a variant of "BlackPOS,"  
 12 a malware strain designed to siphon data from cards when they are swiped at infected  
 13 point-of-sale systems.<sup>19</sup> Hackers had previously utilized BlackPOS in other recent cyber  
 14 attacks, including last year's breach at Target. While many retailers, banks and card  
 15 companies have responded to these recent breaches by adopting technology and security  
 16 practices that help makes transactions and stored data more secure, Home Depot did not  
 17 do so. In light of the breach, however, Home Depot now has announced that it plans to  
 18 have chip-enabled checkout terminals at all of its U.S. stores by the end of 2014.<sup>20</sup>

19 **F. This Data Breach Will Result In Identity Theft and Identity Fraud**

20       48. Home Depot failed to implement and maintain reasonable security  
 21 procedures and practices appropriate to the nature and scope of the Private Information  
 22 compromised in the data breach.

23       49. The ramifications of Home Depot's failure to keep Class members' data  
 24  
 25

---

<sup>18</sup> *Id.*

<sup>19</sup> <http://krebsonsecurity.com/2014/09/home-depot-hit-by-same-malware-as-target/> (last visited September 12, 2014).

<sup>20</sup> <<http://money.msn.com/businessnews/article.aspx?feed=AP&date=20140909&id=17914998&ocid=ansmny11>> (last visited September 12, 2014).

1 secure are severe.

2 50. The information Home Depot compromised, including Plaintiffs' 3 identifying information and/or other financial information, is "as good as gold" to 4 identity thieves, in the words of the Federal Trade Commission ("FTC").<sup>21</sup> Identity theft 5 occurs when someone uses another's personal identifying information, such as that 6 person's name, address, credit card number, credit card expiration dates, and other 7 information, without permission, to commit fraud or other crimes. The FTC estimates 8 that as many as 10 million Americans have their identities stolen each year.

9 51. As the FTC recognizes, once identity thieves have personal information, 10 "they can drain your bank account, run up your credit cards, open new utility accounts, 11 or get medical treatment on your health insurance."<sup>22</sup>

12 52. According to Javelin Strategy and Research, "1 in 4 data breach 13 notification recipients became a victim of identity fraud."<sup>23</sup> Nearly half (46%) of 14 consumers with a breached debit card became fraud victims within the same year.

15 53. Identity thieves can use personal information such as that of Class 16 members, which Home Depot failed to keep secure, to perpetrate a variety of crimes 17 that harm victims. For instance, identity thieves may commit various types of 18 government fraud such as: immigration fraud; obtaining a driver's license or 19 identification card in the victim's name but with another's picture; using the victim's 20 information to obtain government benefits; or filing a fraudulent tax return using the 21 victim's information to obtain a fraudulent refund. Some of this activity may not come 22 to light for years.

---

23 <sup>21</sup> FTC Interactive Toolkit, Fighting Back Against Identity Theft, *available at* 24 *<http://www.dcsheriff.net/community/documents/id-theft-tool-kit.pdf>* (last visited 25 Sept. 12, 2014).

26 <sup>22</sup> FTC, Signs of Identity Theft, *available at* *<http://www.consumer.ftc.gov/articles/0271-signs-identity-theft>* (last visited Sept. 12, 2014).

27 <sup>23</sup> See 2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for 28 Fraudsters, *available at* *<www.javelinstrategy.com/brochure/276>* (last visited Sept. 12, 2014) (the "2013 Identity Fraud Report").

1       54. In addition, identity thieves may get medical services using consumers' 2 compromised personal information or commit any number of other frauds, such as 3 obtaining a job, procuring housing, or even giving false information to police during an 4 arrest.

5       55. It is incorrect to assume that reimbursing a consumer for fraud makes that 6 individual whole again. On the contrary, after conducting a study, the Department of 7 Justice's Bureau of Justice Statistics ("BJS") found that "among victims who had 8 personal information used for fraudulent purposes, 29% spent a month or more 9 resolving problems."<sup>24</sup> In fact, the BJS reported, "resolving the problems caused by 10 identity theft [could] take more than a year for some victims." *Id.* at 11.

11       56. Annual monetary losses from identity theft are in the billions of dollars.

12       57. Javelin Strategy and Research reports that those losses increased to \$21 13 billion in 2013.<sup>25</sup>

14       58. There may be a time lag between when harm occurs versus when it is 15 discovered, and also between when PII or PCD is stolen and when it is used. According 16 to the U.S. Government Accountability Office ("GAO"), which conducted a study 17 regarding data breaches:

18       [L]aw enforcement officials told us that in some cases, *stolen*  
 19 *data may be held for up to a year or more before being used*  
 20 *to commit identity theft.* Further, once stolen data have been  
 21 *sold or posted on the Web, fraudulent use of that information*  
*may continue for years.* As a result, studies that attempt to  
 22 measure the harm resulting from data breaches cannot  
 necessarily rule out all future harm.<sup>26</sup>

23       59. Plaintiffs and Class members now face years of constant surveillance of

24       <sup>24</sup> Victims of Identity Theft, 2012 (Dec. 2013) at 10, available at  
 <<http://www.bjs.gov/content/pub/pdf/vit12.pdf>> (last visited Sept. 12, 2014).

25       <sup>25</sup> See 2013 Identity Fraud Report.

26       <sup>26</sup> GAO, Report to Congressional Requesters, at p.33 (June 2007), available at  
 <<http://www.gao.gov/new.items/d07737.pdf>> (emphases added) (last visited Sept. 12, 2014).

1 their financial and personal records, monitoring, and loss of rights. The Class is  
2 incurring and will continue to incur such damages in addition to any fraudulent credit  
3 and debit card charges incurred by them and the resulting loss of use of their credit and  
4 access to funds, whether or not such charges are ultimately reimbursed by the credit  
5 card companies.

6 **G. Plaintiffs and Class Members Suffered Damages**

7 60. The Data Breach was a direct and proximate result of Home Depot's  
8 failure to properly safeguard and protect Plaintiffs' and Class members' Private  
9 Information from unauthorized access, use, and disclosure, as required by various state  
10 and federal regulations, industry practices, and the common law, including Home  
11 Depot's failure to establish and implement appropriate administrative, technical, and  
12 physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class  
13 members' Private Information to protect against reasonably foreseeable threats to the  
14 security or integrity of such information.

15 61. Plaintiffs' and Class members' Private Information is private and sensitive  
16 in nature and was left inadequately protected by Home Depot. Home Depot did not  
17 obtain Plaintiffs' and Class members' consent to disclose their Private Information to  
18 any other person as required by applicable law and industry standards.

19 62. As a direct and proximate result of Home Depot's wrongful actions and  
20 inaction and the resulting Data Breach, Plaintiffs and Class members have been placed  
21 at an imminent, immediate, and continuing increased risk of harm from identity theft  
22 and identity fraud, requiring them to take the time and effort to mitigate the actual and  
23 potential impact of the Data Breach on their lives including, *inter alia*, by placing  
24 "freezes" and "alerts" with credit reporting agencies, contacting their financial  
25 institutions, closing or modifying financial accounts, and closely reviewing and  
26 monitoring their credit reports and accounts for unauthorized activity.

27 63. Home Depot's wrongful actions and inaction directly and proximately  
28 caused the theft and dissemination into the public domain of Plaintiffs' and Class

1 members' Private Information, causing them to suffer, and continue to suffer, economic  
2 damages and other actual harm for which they are entitled to compensation, including:

- 3 a. theft of their personal and financial information;
- 4 b. the imminent and certainly impending injury flowing from potential  
5 fraud and identify theft posed by their credit/debit card and personal  
6 information being placed in the hands of criminals and already  
7 misused via the sale of Plaintiffs' and Class members' information  
8 on the Internet card black market;
- 9 c. the untimely and inadequate notification of the Data Breach;
- 10 d. the improper disclosure of their Private Information;
- 11 e. loss of privacy;
- 12 f. ascertainable losses in the form of out-of-pocket expenses and the  
13 value of their time reasonably incurred to remedy or mitigate the  
14 effects of the Data Breach;
- 15 g. ascertainable losses in the form of deprivation of the value of their  
16 PII and PCD, for which there is a well-established national and  
17 international market;
- 18 h. overpayments to Home Depot for products purchased during the  
19 Data Breach in that a portion of the price paid for such products by  
20 Plaintiffs and Class members to Home Depot was for the costs of  
21 reasonable and adequate safeguards and security measures that  
22 would protect customers' Private Information, which Home Depot  
23 did not implement and, as a result, Plaintiffs and Class members did  
24 not receive what they paid for and were overcharged by Home  
25 Depot;
- 26 i. the loss of use of and access to their account funds and costs  
27 associated with inability to obtain money from their accounts or  
28 being limited in the amount of money they were permitted to obtain

from their accounts; and

j. deprivation of rights they possess under the California Business and Professions Code § 17200, *et seq.*

64. Plaintiffs also purchased products or services they otherwise would not have purchased, or paid more for those products and services than they otherwise would have paid.

65. Notwithstanding Home Depot's wrongful actions and inaction and the resulting Data Breach, Home Depot has offered consumers only one year of credit monitoring and identity theft protection services. This offer is insufficient because, *inter alia*, it does not address many categories of damages being sought. The cost of adequate and appropriate coverage, or insurance, against the loss position Home Depot has placed Plaintiffs and Class members in, is ascertainable and is a determination appropriate for the trier of fact.

66. Home Depot's offer of one-year of free identity protection services, including credit monitoring, is also insufficient because, as the GAO reported, the PII/PCD could be held by criminals and used to commit fraud after the one year of credit monitoring and identity theft protection expires.

## CLASS ACTION ALLEGATIONS

67. Plaintiffs seek relief in their individual capacity and as representatives of all others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a) and (b)(2) and/or (b)(3), Plaintiffs seek certification of a national class and a California class. The national class is initially defined as follows:

All persons residing in the United States whose personal and/or financial information was disclosed in the data breach affecting Home Depot in 2014 (the “National Class”).

68. The California Class is initially defined as follows:

All persons residing in California whose personal and/or financial information was disclosed in the data breach affecting Home Depot in 2014 (the “California Class).

69. Excluded from each of the above Classes are Home Depot, including any

1 entity in which Home Depot has a controlling interest, is a parent or subsidiary, or  
2 which is controlled by Home Depot, as well as the officers, directors, affiliates, legal  
3 representatives, heirs, predecessors, successors, and assigns of Home Depot. Also  
4 excluded are the judges and court personnel in this case and any members of their  
5 immediate families.

6       70. Numerosity. Fed. R. Civ. P. 23(a)(1). The members of the Class are so  
7 numerous that the joinder of all members is impractical. While the exact number of  
8 Class members is unknown to Plaintiffs at this time, based on information and belief, it  
9 is in the millions.

10     71. Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3). There are questions of  
11 law and fact common to the Class, which predominate over any questions affecting only  
12 individual Class members. These common questions of law and fact include, without  
13 limitation:

- 14       a. Whether Home Depot violated California Civil Code § 1798.81.5 by  
15           failing to implement reasonable security procedures and practices;
- 16       b. Whether Home Depot violated California Civil Code § 1798.82 by failing  
17           to promptly notify class members their personal information had been  
18           compromised;
- 19       c. Whether class members may obtain an injunctive relief against Home  
20           Depot under Civil Code § 1798.84 or under the UCL;
- 21       d. What security procedures and data-breach notification procedure should  
22           Home Depot be required to implement as part of any injunctive relief  
23           ordered by the Court;
- 24       e. Whether Home Depot has an implied contractual obligation to use  
25           reasonable security measures;
- 26       f. Whether Home Depot has complied with any implied contractual  
27           obligation to use reasonable security measures;
- 28       g. What security measures, if any, must be implemented by Home Depot to

1 comply with its implied contractual obligations;

2 h. Whether Home Depot violated California Business and Professions Code §  
 3 17200, *et seq.*; and  
 4 i. The nature of the relief, including equitable relief, to which Plaintiff and  
 5 the Class members are entitled.

6 72. All members of the purposed Classes are readily ascertainable. Home  
 7 Depot has access to addresses and other contact information for millions of members of  
 8 the Classes, which can be used for providing notice to many Class members.

9 73. Typicality. Fed. R. Civ. P. 23(a)(3). Plaintiffs' claims are typical of those  
 10 of other Class members because Plaintiffs' information, like that of every other class  
 11 member, was misused and/or disclosed by Home Depot.

12 74. Adequacy of Representation. Fed. R. Civ. P. 23(a)(4). Plaintiffs will  
 13 fairly and adequately represent and protect the interests of the members of the Class.  
 14 Plaintiffs' Counsel are competent and experienced in litigating class actions.

15 75. Superiority of Class Action. Fed. R. Civ. P. 23(b)(3). A class action is  
 16 superior to other available methods for the fair and efficient adjudication of this  
 17 controversy since joinder of all the members of the Class is impracticable.  
 18 Furthermore, the adjudication of this controversy through a class action will avoid the  
 19 possibility of inconsistent and potentially conflicting adjudication of the asserted  
 20 claims. There will be no difficulty in the management of this action as a class action.

21 76. Damages for any individual class member are likely insufficient to justify  
 22 the cost of individual litigation, so that in the absence of class treatment, Home Depot's  
 23 violations of law inflicting substantial damages in the aggregate would go un-remedied  
 24 without certification of the Class.

25 77. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and  
 26 (b)(2), because Home Depot has acted or has refused to act on grounds generally  
 27 applicable to the Class, so that final injunctive relief or corresponding declaratory relief  
 28 is appropriate as to the Class as a whole.

## COUNT I

## For Violation of the Civil Code Sections 1798.81.5 & 1798.82

## **(On Behalf of Plaintiffs and the California Class)**

78. Plaintiffs incorporate the substantive allegations contained in Paragraphs 1 through 77 as if fully set forth herein.

79. “[T]o ensure that personal information about California residents is protected,” the California legislature enacted Civil Code section 1798.81.5, which requires that any business that “owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.”

80. By failing to implement reasonable measures to protect the California Class's personal information, Home Depot violated Civil Code section 1798.81.5.

81. In addition, by failing to promptly notify all affected Home Depot users that their personal information had been acquired (or was reasonably believed to have been acquired) by unauthorized persons in the data breach, Home Depot violated Civil Code Section 1798.82 of the same title.

82. As a direct or proximate result of Home Depot's violations of Civil Code Sections 1798.81.5 and 1798.82, Plaintiffs and Class members were (and continue to be) injured and have suffered (and will continue to suffer) the damages described in detail in Paragraphs 60 through 66 of this Class Action Complaint.

83. In addition, by violating Civil Code Sections 1798.81.5 and 1798.82, Home Depot “may be enjoined” under Civil Code Section 1798.84(e).

84. Home Depot's violations of Civil Code Section 1798.81.5 and 1798.82 also constitute an unlawful acts or practices under California's Unfair Competition Law (UCL), Cal. Bus. & Prof. Code § 17200 et seq., which affords the Court discretion to enter whatever orders may be necessary to prevent future unlawful acts or practices.

85. Plaintiffs accordingly request that the Court enter an injunction requiring

1 Home Depot to implement and maintain reasonable security procedures, including, but  
2 not limited to: (1) ordering that Home Depot utilize strong industry standard encryption  
3 algorithms for encryption keys that provide access to stored customer data; (2) ordering  
4 that Home Depot implement the use of its encryption keys in accordance with industry  
5 standards; (3) ordering that Home Depot, consistent with industry standard practices,  
6 engage third party security auditors/penetration testers as well as internal security  
7 personnel to conduct testing, including simulated attacks, penetration tests and audits on  
8 Home Depot's systems on a periodic basis; (4) ordering that Home Depot engage third  
9 party security auditors and internal personnel, consistent with industry standard  
10 practices, to run automated security monitoring; (5) ordering that Home Depot audit,  
11 test and train its security personnel regarding any new or modified procedures; (6)  
12 ordering that Home Depot, consistent with industry standard practices, segment  
13 consumer data by, among other things, creating firewalls and access controls so that if  
14 one area of Home Depot is compromised, hackers cannot gain access to other portions  
15 of Home Depot's systems; (7) ordering that Home Depot purge, delete, destroy in a  
16 reasonable secure manner customer data not necessary for its provisions of services;  
17 (8); ordering that Home Depot, consistent with industry standard practices, conduct  
18 regular database scanning and security checks; (9) ordering that Home Depot,  
19 consistent with industry standard practices, evaluate web applications for vulnerabilities  
20 to prevent web application threats to consumers who purchase Home Depot products  
21 and services through the internet; (10) ordering that Home Depot, consistent with  
22 industry standard practices, periodically conduct internal training and education to  
23 inform internal security personnel how to identify and contain a breach when it occurs  
24 and what to do in response to a breach; and (11) ordering Home Depot to meaningfully  
25 educate its customers about the threats they face as a result of the loss of their PII/PCD  
26 to third parties, as well as the steps Home Depot's customers must take to protect  
27 themselves.

28 86. Plaintiffs further request that the Court requires Home Depot to identify

1 and notify all members of the Class who have not yet been informed of the Data  
2 Breach, and to notify affected customers of any future data breaches by email within 24  
3 hours of Home Depot's discovery of a breach or possible breach and by mail within 72  
4 hours.

5 **COUNT II**

6 **Breach of Implied Contract**

7 **(On Behalf of Plaintiffs, the National Class, and the California Class)**

8 87. Plaintiffs incorporate the substantive allegations contained in Paragraphs 1  
9 through 77 as if fully set forth herein.

10 88. Home Depot solicited and invited Plaintiffs and Class members to  
11 purchase products at Home Depot's stores using their credit or debit cards. Plaintiffs  
12 and Class members accepted Home Depot's offers and used their credit or debit cards to  
13 purchase products at Home Depot's stores during the period of the Data Breach.

14 89. When Plaintiffs and Class members provided their PII and PCD to Home  
15 Depot to make purchases at Home Depot's stores, including but not limited to the PII  
16 and PCD contained on the face of, and embedded in the magnetic strip of, their debit  
17 and credit cards, Plaintiffs and Class members entered into implied contracts with  
18 Home Depot pursuant to which Home Depot agreed to safeguard and protect such  
19 information and to timely and accurately notify Plaintiffs and Class members if their  
20 data had been breached and compromised.

21 90. Each purchase at a Home Depot store made by Plaintiffs and Class  
22 members using their credit or debit card was made pursuant to the mutually agreed-  
23 upon implied contract with Home Depot under which Home Depot agreed to safeguard  
24 and protect Plaintiffs' and Class members' PII and PCD, including all information  
25 contained in the magnetic stripe of Plaintiffs' and Class members' credit or debit cards,  
26 and to timely and accurately notify them if such information was compromised or  
27 stolen.

28 91. Plaintiffs and Class members would not have provided and entrusted their

1 PII and PCD, including all information contained in the magnetic stripes of their credit  
 2 and debit cards, to Home Depot to purchase products at Home Depot's stores in the  
 3 absence of the implied contract between them and Home Depot.

4 92. Plaintiffs and Class members fully performed their obligations under the  
 5 implied contracts with Home Depot.

6 93. Home Depot breached the implied contracts it made with Plaintiffs and  
 7 Class members by failing to safeguard and protect the PII and PCD of Plaintiffs and  
 8 Class members and by failing to provide timely and accurate notice to them that their  
 9 PII and PCD was compromised in and as a result of the Data Breach.

10 94. As a direct and proximate result of Home Depot's breaches of the implied  
 11 contracts between Home Depot and Plaintiffs and Class members, Plaintiffs and Class  
 12 members sustained actual losses and damages as described in detail in Paragraphs 60  
 13 through 66 of this Class Action Complaint.

14 **COUNT III**

15 **Violation of California Unfair Competition Law, Bus. & Prof. Code § 17200, *et seq.***  
 16 **(On Behalf of Plaintiffs and the California Class)**

17 95. Plaintiffs incorporate the substantive allegations contained in Paragraphs 1  
 18 through 77 as if fully set forth herein.

19 96. Home Depot engaged in unfair, fraudulent and unlawful business practices  
 20 in violation of the Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq.*  
 21 (“UCL”).

22 97. Plaintiffs suffered injury in fact and lost money or property as a result of  
 23 Home Depot's alleged violations of the UCL.

24 98. The acts, omissions and conduct of Home Depot as alleged constitutes a  
 25 “business practice” within the meaning of the UCL.

26 99. Home Depot violated the unlawful prong of the UCL by violating Civil  
 27 Code Sections 1798.81.5 and 1798.82, as alleged above.

28 100. Home Depot also violated the unlawful prong of the UCL by failing to

1 honor the terms of the implied contracts between Plaintiffs and Class members and  
2 Home Depot, as alleged above.

3       101. Home Depot's acts, omissions and conduct also violate the unfair prong of  
4 the UCL because Home Depot's acts, omissions and conduct, as alleged herein,  
5 offended public policy and constitutes immoral, unethical, oppressive, and  
6 unscrupulous activities that caused substantial injury, including to Plaintiffs and other  
7 Class members. The gravity of Home Depot's conduct outweighs any potential benefits  
8 attributable to such conduct and there were reasonably available alternatives to further  
9 Home Depot's legitimate business interests, other than Home Depot's conduct  
10 described herein.

11       102. Home Depot's conduct also undermines California public policy — as  
12 reflected in statutes like the Information Practices Act, Cal. Civ. Code § 1798 *et seq.*,  
13 and the California Customer Records Act, Cal. Civ. Code §§ 1798.81.5 and 1798.82  
14 concerning customer records — which seek to protect customer data and ensure that  
15 entities who solicit or are entrusted with personal data utilize reasonable security  
16 measures.

17       103. By failing to disclose that it does not enlist industry standard security  
18 practices, which render Home Depot's products and services particularly vulnerable to  
19 data breaches, Home Depot engaged in a fraudulent business practice that is likely to  
20 deceive a reasonable consumer.

21       104. A reasonable consumer would not have purchased a product at a Home  
22 Depot store with a credit or debit card had she known the truth about Home Depot's  
23 security procedures. By withholding material information about Home Depot's security  
24 practices, Home Depot was able to convince customers to provide and entrust their  
25 Private Information to Home Depot. Had Plaintiffs known truth about Home Depot's  
26 security procedures, they would not have made purchases at Home Depot, or would not  
27 have paid as much for them.

28       105. Home Depot's failure to disclose that it does not enlist industry standard

1 security practices also constitutes an unfair business practice under the UCL. Home  
2 Depot's conduct is unethical, unscrupulous, and substantially injurious to the California  
3 Class. Whereas Home Depot's competitors have spent the time and money necessary to  
4 appropriately safeguard their products, service, and customer information, Home Depot  
5 has not—to the detriment of its customers and to competition.

6 106. As a result of Home Depot's violations of the UCL, Plaintiffs and the other  
7 members of the Contract Class are entitled to injunctive relief including, but not limited  
8 to: (1) ordering that Home Depot utilize strong industry standard encryption algorithms  
9 for encryption keys that provide access to stored customer data; (2) ordering that Home  
10 Depot implement the use of its encryption keys in accordance with industry standards;  
11 (3) ordering that Home Depot, consistent with industry standard practices, engage third  
12 party security auditors/penetration testers as well as internal security personnel to  
13 conduct testing, including simulated attacks, penetration tests and audits on Home  
14 Depot's systems on a periodic basis; (4) ordering that Home Depot engage third party  
15 security auditors and internal personnel, consistent with industry standard practices, to  
16 run automated security monitoring; (5) ordering that Home Depot audit, test and train  
17 its security personnel regarding any new or modified procedures; (6) ordering that  
18 Home Depot, consistent with industry standard practices, segment consumer data by,  
19 among other things, creating firewalls and access controls so that if one area of Home  
20 Depot is compromised, hackers cannot gain access to other portions of Home Depot's  
21 systems; (7) ordering that Home Depot purge, delete, destroy in a reasonable secure  
22 manner customer data not necessary for its provisions of services; (8); ordering that  
23 Home Depot, consistent with industry standard practices, conduct regular database  
24 scanning and security checks; (9) ordering that Home Depot, consistent with industry  
25 standard practices, evaluate web applications for vulnerabilities to prevent web  
26 application threats to consumers who purchase Home Depot products and services  
27 through the internet; (10) ordering that Home Depot, consistent with industry standard  
28 practices, periodically conduct internal training and education to inform internal

1 security personnel how to identify and contain a breach when it occurs and what to do  
 2 in response to a breach; and (11) ordering Home Depot to meaningfully educate its  
 3 customers about the threats they face as a result of the loss of their PII to third parties  
 4 and the theft of Home Depot's source code, as well as the steps Home Depot's  
 5 customers must take to protect themselves.

6 107. As a result of Home Depot's violations of the UCL, Plaintiffs and Class  
 7 members have suffered injury in fact and lost money or property, as detailed in  
 8 Paragraphs 60 through 66 of this Class Action Complaint. They purchased products or  
 9 services they otherwise would not have purchased, or paid more for those products and  
 10 services than they otherwise would have paid. Plaintiffs request that the Court issue  
 11 sufficient equitable relief to restore Class members to the position they would have been  
 12 in had Home Depot not engaged in unfair competition, including by ordering restitution  
 13 of all funds that Home Depot may have acquired as a result of its unfair competition.

14 **REQUEST FOR RELIEF**

15 WHEREFORE, Plaintiffs, individually and on behalf of all Class members  
 16 proposed in this Complaint, respectfully requests that the Court enter judgment in their  
 17 favor and against Home Depot, as follows:

18 A. For an Order certifying this action as a class action and appointing  
 19 Plaintiffs and their Counsel to represent the Class;

20 B. For equitable relief enjoining Home Depot from engaging in the wrongful  
 21 conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs  
 22 and Class members' private information, and from refusing to issue prompt, complete  
 23 and accurate disclosures to the Plaintiffs and Class members;

24 C. For equitable relief compelling Home Depot to utilize appropriate methods  
 25 and policies with respect to consumer data collection, storage and safety and to disclose  
 26 with specificity to Class members the type of PII and PCD compromised, and other  
 27 information required under Cal. Civ. Code § 1798.82;

28 D. For equitable relief requiring restitution and disgorgement of the revenues

1 wrongfully retained as a result of Home Depots' wrongful conduct;

2 E. For an award of actual damages, compensatory damages, statutory  
3 damages, and statutory penalties, in an amount to be determined;

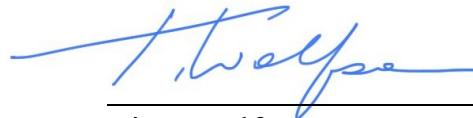
4 F. For an award of costs of suit and attorneys' fees, as allowable by law; and

5 G. Such other and further relief as this court may deem just and proper.

6 Dated: September 12, 2014

7 Respectfully submitted,

8 **AHDOOT & WOLFSON, PC**

9 

10 \_\_\_\_\_  
11 Tina Wolfson  
12 Robert Ahdoot  
13 Theodore W. Maya  
14 Bradley King  
15 Keith Custis (Of Counsel)  
16 AHDOOT & WOLFSON, PC  
17 10850 Wilshire Blvd., Suite 370  
18 Los Angeles, California 90024  
19 Telephone: 310-474-9111  
20 Facsimile: 310-474-8585

21 JOHN A. YANCHUNIS  
22 MORGAN & MORGAN  
23 COMPLEX LITIGATION GROUP  
24 201 N. Franklin Street, 7th Floor  
25 Tampa, Florida 33602  
26 Telephone: (813) 223-5505  
27 Facsimile: (813) 223-5402

28 PAUL C. WHALEN  
29 LAW OFFICES OF PAUL C. WHALEN, P.C.  
30 768 Plandome Road  
31 Manhasset, New York 11030  
32 Telephone: (516) 627-5610  
33 Facsimile: (212) 658-9685

34 Counsel for Plaintiffs  
35 WALID KHALAF, JASMIN GONZALEZ,  
36 STEFANIE SMITH and STEVEN O'BRIEN